

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MASSACHUSETTS**

ALICIA SHILLITO, *individually and on
behalf of herself and all others similarly
situated*,

and

PARKER MEDICAL CENTER LPD,
*individually and on behalf of itself and all others
similarly situated*,

Plaintiffs,

v.

**CHANGE HEALTHCARE INC.,
UNITEDHEALTH GROUP INC.,
UNITEDHEALTHCARE INC., and
OPTUM INC.**,

Defendants.

Case No.

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiff Alicia Shillito and Plaintiff Parker Medical Center LPD (collectively “Plaintiffs”) brings this Class Action Complaint, individually and on behalf of all others similarly situated (the “Class Members”), against Defendants Change Healthcare Inc. (“Change”), UnitedHealth Group Inc. (“UnitedHealth”), UnitedHealthcare Inc. (“UnitedHealthcare”), and Optum Inc. (“Optum,” and collectively with Change, UnitedHealth, and UnitedHealthcare, “Defendants”) and allege as follows, based upon information and belief, investigation of counsel, and the personal knowledge of Plaintiffs.

NATURE OF CASE

1. This class action arises out of the recent targeted cyberattack and data breach where unauthorized third-party criminals retrieved and exfiltrated the highly-sensitive consumer data of millions of Americans, as a result of the Defendants’ failure to reasonably and adequately secure

this highly-sensitive consumer data (the “Data Breach”). At a recent hearing before the United States Senate, Senator Mike Crapo described the attack as “by far the most disruptive cyberattack on the health care industry to date.”¹

2. Change is a “health tech giant” and is a subsidiary of UnitedHealth Group’s Optum division, providing payment and revenue cycle services, clinical and imaging services, and patient and member engagement services to healthcare providers. Change is the nation’s largest healthcare clearing house, processing \$1.5 trillion in medical claims annually. Change specializes in moving patient data between doctors’ offices and/or insurance companies, including medical bills and records for patients serviced by Plaintiffs and Class Members containing patients’ sensitive diagnoses, treatment, and histories that “reveal everything from abortions to mental health disorders to diagnosis of cancer to sexually transmitted infections.” During a recent congressional Hearing concerning the Data Breach, U.S. Senator Ron Wyden, stated that Change “processes roughly 15 billion health care transactions annually, and a third of Americans’ patient records pass through its digital doors.”²

3. During the regular course of conducting its daily business, Change acquires, collects, and stores consumers’ personal data, including personally identifying information (“PII”) and protected health information (“PHI”) (collectively, “Private Information”).

4. On February 21, 2024, UnitedHealth Group, the nation’s largest insurer, filed a Form 8-K with the Securities and Exchange Commission disclosing that Change’s systems had been infiltrated by a “suspected nation-state associated cyber security threat actor.”³ Companies,

¹ Crapo Statement at Hearing on Change Healthcare Cyberattack, U.S. Senate Committee on Finance, Hacking America’s Health Care: Assessing the Change Healthcare Cyber Attack and What’s Next (May 1, 2024), https://www.finance.senate.gov/imo/media/doc/0501_crapo_statement.pdf (emphasis added)

² *Id.*

³ UNITED STATES SECURITIES AND EXCHANGE COMMISSION: Form 8-K, UNITEDHEALTH GROUP INCORPORATED (Feb. 21, 2024), <https://www.sec.gov/Archives/edgar/data/731766/000073176624000045/unh->

such as UnitedHealth Group, are required to file Form 8-K to announce major events that shareholders should know about.

5. The Form 8-K documented what was later claimed, on February 28, 2024, by the notorious ransomware cybercriminals, known as the BlackCat/ALPHV ransomware group (“BlackCat”), that the Data Breach, was a successful infiltration by BlackCat into Defendants’ inadequately protected network allowing access to highly sensitive information, including Private Information, which was being kept unprotected.⁴

6. Reports indicate the attack was carried out as a ransomware attack in which BlackCat accessed multiple terabytes of sensitive health data to secure a \$22 million ransom payment from Change, which, upon information and belief, was paid in the Spring of 2024. In a statement made by UnitedHealth Group, BlackCat took files containing Private Information that it says may “cover a substantial proportion of people in America.”⁵

7. At a recent Senate hearing, the Data Breach was described as “the biggest cybersecurity disruption to health care in American history.”⁶

8. In the wake of the targeted cyberattack, Defendant UnitedHealth Group disconnected Defendant Change from the rest of its healthcare systems and networks. For weeks, Change was offline leaving healthcare providers, such as Plaintiffs and Class Members, in a state

20240221.htm

⁴ Sergiu Gatlan, Ransomware Gang Claims They Stole 6TB of Change Healthcare Data, BleepingComputer (Feb 28, 2024), <https://www.bleepingcomputer.com/news/security/ransomware-gang-claims-they-stole-6tb-of-change-healthcare-data/>.

⁵ Zach Whittaker, UnitedHealth says Change hackers stole health data on ‘substantial proportion of people in America’, TechCrunch (Apr. 22, 2024) <https://techcrunch.com/2024/04/22/unitedhealth-change-healthcare-hackers-substantial-proportion-americans/>.

⁶ , U.S. Senate Committee on Finance, Hacking America’s Health Care: Assessing the Change Healthcare Cyber Attack and What’s Next (May 1, 2024)

of what U.S. Senator Ron Wyden described as “financial bedlam.”⁷ For several months following the Data Breach, the doctors, hospitals, and other small providers providing the health care on the front end of those 15 billion annual transactions frequently had to draw from their personal resources just to survive because, as a result of Defendants’ security failures, insurance companies were unable or unwilling to reimburse these front end providers.

9. At the time of this filing and over two months after the Data Breach was reported by Defendants, Plaintiffs and Class Members have still been left in the dark about how long Defendants’ systems outage affecting their business and livelihood would last.

10. Although it is still early following the Data Breach and we do not yet know the full extent of the damage, the currently known fallout from the Data Breach has been far-reaching across the healthcare system in the United States, including, *inter alia*, causing severe disruptions to Plaintiffs’ and Class Members’ ability to process and be reimbursed for claims, and to check patients’ eligibility for treatment.⁸

11. An American Hospital Association survey found that more than 90 percent of hospitals were financially impacted by the cyberattack, with more than 70 percent reporting that the outage had directly affected their ability to care for patients.⁹

12. Plaintiffs and Class Members are still feeling the impacts of the Data Breach as they struggle to run their practices amid reduced cash flows that threaten to permanently shutter

⁷ Wyden Hearing Statement on Change Healthcare Cyberattack and UnitedHealth Group’s Response, U.S. Senate Committee on Finance, Hacking America’s Health Care: Assessing the Change Healthcare Cyber Attack and What’s Next (May 1, 2024), https://www.finance.senate.gov/imo/media/doc/0501_wyden_statement.pdf

⁸ Outages from Change Healthcare cyberattack causing financial ‘mess’ for doctors, NBC, <https://www.nbcnews.com/news/us-news/outages-change-healthcarecyberattack-causing-financial-mess-doctors-rena141321> (Mar. 1, 2024).

⁹ Crapo Statement at Hearing on Change Healthcare Cyberattack, U.S. Senate Committee on Finance, Hacking America’s Health Care: Assessing the Change Healthcare Cyber Attack and What’s Next (May 1, 2024), https://www.finance.senate.gov/imo/media/doc/0501_crapo_statement.pdf (emphasis added)

their doors, and the specter of permanent discontinuation of the vital services their patients rely on.

13. Defendants are subject to HIPAA's privacy rules as healthcare business associates because they knowingly obtain, collect, and store patient Private Information. Defendants, therefore, have a duty to secure, maintain, protect, and safeguard the Private Information in their possession against unauthorized access and disclosure through reasonable and adequate data security measures. Based on numerous prior cyberattacks exfiltrating highly sensitive healthcare information and resulting ransoms, at the time of the Data Breach, Defendants were well-aware that Private Information is extremely valuable to cybercriminals, which made it highly foreseeable that Defendants, the nation's largest health insurers, would be the target of a cyberattack. As Senator Mike Crapo recently described: "While the February hack on Change was by far the most disruptive cyberattack on the health care industry to date, *it was certainly not the first*. According to a report by the Federal Bureau of Investigation, the health care sector experienced more ransomware attacks than any other critical infrastructure sector in 2023."¹⁰

14. Defendants owed non-delegable duties to Plaintiffs and Class Members to protect and safeguard the Private Information and to implement reasonable and adequate security measures to ensure they could administer and provide the services they contracted to provide to Plaintiffs and Class Members in a manner uninterrupted by foreseeable risks the Defendant failed to reasonably and adequately prepare for. Defendants' failure to do so directly resulted in a Data Breach of "unprecedented magnitude" and significant disruption to the healthcare system across the United States.

¹⁰ Crapo Statement at Hearing on Change Healthcare Cyberattack, U.S. Senate Committee on Finance, Hacking America's Health Care: Assessing the Change Healthcare Cyber Attack and What's Next (May 1, 2024), https://www.finance.senate.gov/imo/media/doc/0501_crapo_statement.pdf (emphasis added)

15. Defendants' failure to do so is particularly galling in light of the fact that UnitedHealthcare itself had already recently been targeted by cybercriminals who accessed and exfiltrated patients' highly-sensitive information via a UnitedHealthcare broker portal.¹¹ In a September 1, 2023 statement to affected individuals, UnitedHealthcare stated, "UCH is committed to protecting our members' and brokers' information and maintaining the integrity of our systems."¹² Despite these outward assurances and knowing they were a target of cybercriminals, Defendants continued to fail to adequately safeguard the sensitive Private Information it collected and maintained.

16. Defendants maintained and shared the Private Information in a negligent and/or reckless manner. In particular, Private Information was maintained on computer systems in a condition vulnerable to cyberattacks that lacked, for example, multi-factor authentication to access.

17. Plaintiffs' and Class Members' ability to effectively deliver critical medical services without themselves teetering on financial ruin has been severely compromised due to Defendants' negligent and/or reckless acts and omissions and Defendants' repeated failure to reasonably and adequately protect Private Information.

18. Accordingly, Plaintiffs bring this action against Defendants, seeking redress for Defendants' unlawful conduct and asserting claims for: (i) negligence; (ii) breach of implied contract; (iii) breach of third-party beneficiary contracts; and (iv) unjust enrichment. Through these claims, Plaintiffs seek damages in an amount to be proven at trial, as well as injunctive and

¹¹ United Health Care Notification to Affected Individuals of Data Security Incident, <https://cms.member.myuhc.com/content/dam/iex/assets/pdf/Jarvis%20Website%20posting%20.pdf> (last accessed May 14, 2024)

¹² *Id.*

other equitable relief, including reasonable and adequate improvements to Defendants' data security systems, policies, and practices, implementation of annual audits reviewing the same, and adequate reimbursement for all Class Members for the financial injuries suffered as a result of the Data Breach and ensuing services outage.

THE PARTIES

19. Plaintiff Alicia Shillito is a natural person, resident, and citizen of the State of Arizona. Plaintiff Shillito is the co-owner, office manager, and authorized representative of Parker Medical Center LPD.

20. Plaintiff Parker Medical Center LPD, is a family medical practice with its principal place of business in Parker, Arizona.

21. Defendant Change is a Delaware corporation with its principal place of business located at 424 Church Street, Suite 1400, Nashville, Tennessee 37219. Defendant Change is a part of Defendant Optum, and works across the health system to enable information, claims, and payments to flow between physicians, pharmacists, health plans and governments. UnitedHealth Group acquired Change in or around 2022.

22. Defendant UnitedHealth Group is a Delaware corporation with its principal place of business at 9900 Bren Road East, Minnetonka, Minnesota 55343. UnitedHealth Group operates and maintains several offices in Tennessee, including in Brentwood, Lenoir City, Kingston, Maryville, Columbia, Cordova, Smyrna, Gallatin, and Nashville.

23. Defendant UnitedHealthcare is a Delaware corporation with its principal place of business at 9900 Bren Road East, Minnetonka, Minnesota 55343. UnitedHealthcare is the insurance benefits arm of Defendant UnitedHealth Group.

24. Defendant Optum is a Delaware corporation with its principal place of business at

9900 Bren Road East, Minnetonka, Minnesota. Optum “delivers care aided by technology and data, empowering people, partners and providers with the guidance and tools they need to achieve better health.”¹³ UnitedHealth Group acquired Optum in or around 2011.

JURISDICTION AND VENUE

25. This Court has original jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2) because Plaintiffs, and at least one member of the putative Class, as defined below, is a citizen of a different state than Defendants, there are more than 100 putative class members, and the amount in controversy exceeds \$5 million exclusive of interest and costs.

26. This Court has general personal jurisdiction over Defendants because Defendant Change has its principal place of business in this district, and all Defendants operate in and direct commerce at this District.

27. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because Defendant Change’s principal place of business is located in this District, a substantial part of the events giving rise to this action occurred in this District, and Defendants have harmed Class Members residing in this District.

FACTUAL ALLEGATIONS

Defendants’ Businesses

28. UnitedHealth Group is the largest healthcare insurer in the United States, and the fifth largest company in the United States.¹⁴ Overall, UnitedHealth Group reaches 152 million individuals across all arms of its business, from insurance, to physician practices, to home health

¹³ Optum: Technology and data-enabled care delivery, UnitedHealth Group, <https://www.unitedhealthgroup.com/people-and-businesses/businesses/optum.html> (last accessed May 9, 2024).

¹⁴ Wyden Hearing Statement on Change Healthcare Cyberattack and UnitedHealth Group’s Response, U.S. Senate Committee on Finance, Hacking America’s Health Care: Assessing the Change Healthcare Cyber Attack and What’s Next (May 1, 2024), https://www.finance.senate.gov/imo/media/doc/0501_wyden_statement.pdf.

and pharmacy. In 2023 alone, UnitedHealth Group generated \$324 billion in revenue.¹⁵

29. Change is a “health tech giant”¹⁶ and is a subsidiary of UnitedHealth Group’s Optum division, providing payment and revenue cycle services, clinical and imaging services, and patient and member engagement services to healthcare providers.¹⁷ Change is the nation’s largest healthcare clearing house, processing \$1.5 trillion in medical claims annually.¹⁸ Change specializes in moving patient data between doctors’ offices and/or insurance companies, including medical bills and records containing sensitive diagnoses, treatment, and histories that “reveal everything from abortions to mental health disorders to diagnosis of cancer to sexually transmitted infections.”¹⁹ And, according to the recent testimony of U.S. Senator Ron Wyden, Change “processes roughly 15 billion health care transactions annually, and a third of Americans’ patient records pass through its digital doors.”²⁰

30. Plaintiffs and Class Members are current or former medical providers who used Defendants’ services.

31. In the course of facilitating insurance and other transactions related to Plaintiffs’ and Class Members’ healthcare businesses, Defendants receive, create, and handle patient Private

¹⁵ *Id.*

¹⁶ Zach Whittaker, UnitedHealth says Change hackers stole health data on ‘substantial proportion of people in America’, TechCrunch (Apr. 22, 2024) <https://techcrunch.com/2024/04/22/unitedhealth-change-healthcare-hackers-substantial-proportion-americans/>.

¹⁷ What We Do, Change Healthcare: Part of Optum, <https://www.changehealthcare.com/> (last accessed May 9, 2024).

¹⁸ Crapo Statement at Hearing on Change Healthcare Cyberattack, U.S. Senate Committee on Finance, Hacking America’s Health Care: Assessing the Change Healthcare Cyber Attack and What’s Next (May 1, 2024), https://www.finance.senate.gov/imo/media/doc/0501_crapo_statement.pdf

¹⁹ Wyden Hearing Statement on Change Healthcare Cyberattack and UnitedHealth Group’s Response, U.S. Senate Committee on Finance, Hacking America’s Health Care: Assessing the Change Healthcare Cyber Attack and What’s Next (May 1, 2024), https://www.finance.senate.gov/imo/media/doc/0501_wyden_statement.pdf.

²⁰ *Id.*

Information. Indeed, to receive services from Defendants, Plaintiffs and Class Members' patients were required to provide highly sensitive Private Information, including some or all the following:

- Full names and addresses;
- Personal email addresses and phone numbers;
- Dates of birth;
- Social Security numbers;
- Driver's licenses (or other similar state identifications);
- Health insurance information;
- Health information including but not limited to information about diagnosis and treatment, personal medical history, family medical history, mental health information, information related to STDs and treatment, information related to abortions, medication information, and medical record numbers;
- Information about physicians and related medical professionals who had been involved in previous or ongoing treatment of the patient;
- Billing and claims information including but not limited to information related to credit and debit card numbers, bank account statements and account numbers, and insurance payment details;
- Medicare/Medicaid information;
- Medication information;
- Diagnostic results and treatment information.

32. This sort of Private Information is extremely sensitive and is extremely valuable to criminals because it can be used to commit serious identity and medical identity theft crimes.

33. In light of the quantity and sensitive nature of the Private Information it stores,

Change promulgated a privacy policy describing how it used and disclosed confidential and personal information including claiming that “We implement and maintain organizational, technical, and administrative *security measures designed to safeguard the data we process against unauthorized access*, destruction, loss, alteration, or misuse. These measures are aimed at providing on-going integrity and *confidentiality of data, including your personal information*.”²¹

34. Because of the highly sensitive and personal nature of the information Defendants acquire, store, and transfer with respect to consumers and other individuals, Defendants must: keep Private Information private; comply with healthcare industry standards related to data security and Private Information, including FTC guidelines; inform consumers of their legal duties and comply with all federal and state laws protecting consumer Private Information; only use and release Private Information for reasons that relate to the products and services delivered by Plaintiffs and Class Members obtained from Defendants and provide adequate notice to individuals if their Private Information is disclosed without authorization.

35. As HIPAA covered business entities, as discussed *infra*, Defendants are required to implement adequate safeguards to prevent unauthorized use or disclosure of Private Information, including by implementing the requirements of the HIPAA Security Rule and to report any unauthorized use or disclosure of Private Information, including incidents that constitute breaches of unsecured PHI, as in the case of the Data Breach complained of herein.

36. However, despite the existence of these duties, Defendants did not maintain adequate security to protect their systems from infiltration by cybercriminals, resulting in a massive disruption to the U.S. healthcare system, including to Plaintiffs’ and Class Members’ ability to deliver vital healthcare services to patients.

²¹ Change Healthcare: Part of Optum, Privacy at Change Healthcare, <https://www.changehealthcare.com/privacy-notice> (last accessed May 15, 2024).

37. Contrary to Defendants' representations, Defendants failed to implement adequate data security measures, as evidenced by Defendants' admission of the Data Breach, which affected, by some estimates, one-third of all Americans.²²

Defendants are Covered Entities Subject to HIPAA

38. Defendants are "business associates" of healthcare providers and covered entities under HIPAA, each of whom provide healthcare, medication, and insurance related services to hundreds of millions of patients annually either directly or via their healthcare clients. As a regular and necessary part of their businesses, Defendants collect, store, and transfer the highly sensitive Private Information of patients.

39. As covered entities, Defendants are required under federal and state law to maintain the strictest confidentiality of the Private Information they acquire, receive, collect, transfer, and store. Defendants are further required to maintain sufficient safeguards to protect that Private Information from being accessed by unauthorized third parties.

40. Due to the nature of Defendants' businesses, which includes providing a range of revenue cycle, insurance, technology, and financial services to healthcare clients, including obtaining, storing, and maintaining electronic health and medical records, Defendants would be unable to engage in their regular business activities without collecting and aggregating Private Information they know and understand to be sensitive and confidential.

41. In fact, whenever Defendants contract with covered entities (healthcare providers such as Plaintiffs and Class Members) to provide various business and medical services, HIPAA requires that these contracts mandate that Defendants will use adequate safeguards to prevent

²² Testimony of Andrew Witty Chief during the U.S. Senate Committee on Finance, Hacking America's Health Care: Assessing the Change Healthcare Cyber Attack and What's Next (May 1, 2024).

unauthorized use or disclosure of PHI, including by implementing the HIPAA Security Rule²³ and immediately reporting any unauthorized use or disclosure of PHI (such as the Data Breach) to affected covered entities.

42. For its part, Defendant Change explicitly touts its “Commitment to Compliance,” claiming that it “provides assurance to our customers that applicable Change Healthcare products and services meet or exceed regulatory requirements.”²⁴

43. By obtaining, collecting, using, and deriving a benefit from Private Information, Defendants assumed legal and equitable duties and knew or should have known that they were responsible for protecting Private Information from unauthorized disclosure.

44. Plaintiffs and Class Members are or were healthcare providers with whom Defendants contracted, whose patients’ Private Information was maintained by Defendants and directly or indirectly entrusted Defendants with their Private Information.

45. Plaintiffs and Class Members relied on Defendants to implement and follow adequate data security policies and protocols, to keep their patients’ Private Information confidential and securely maintained, to use such Private Information solely for business and healthcare purposes, and to prevent unauthorized disclosures of Private Information. Plaintiffs and Class Members reasonably expected that Defendants would safeguard and keep Private Information confidential to, *inter alia*, ensure the orderly and efficient delivery and reimbursement for healthcare services provided by Plaintiffs and Class Members.

46. As described throughout this Complaint, Defendants failed to reasonably and

²³ The HIPAA Security Rule establishes national standards to protect individuals’ electronic personal health information that is created, received, used, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information. See 45 C.F.R. Part 160 and Part 164, Subparts A and C

²⁴ HIPAA Simplified, Change Healthcare, <https://support.changehealthcare.com/customer-resources/hipaa-simplified> (last accessed May 7, 2024).

adequately protect, secure, and/or store Private Information prior to, during, or after the Data Breach, but rather, enacted unreasonable data security measures they knew or should have known were insufficient to reasonably protect the highly sensitive Private Information that they maintained. Consequently, cybercriminals circumvented Defendants' security measures, resulting in a significant Data Breach.

The Data Breach of Defendants' Systems

47. Beginning on or around February 21, 2024, the notorious BlackCat ransomware group exploited the Defendants' failure to adequately and reasonably safeguard their data systems, and accessed, copied, and stole Plaintiffs' and Class Members' patients' Private Information that was processed and stored on Defendant Change's servers and networks.

48. In an online notice published to its website, on or around February 21, 2024 (the "Online Notice"), Defendant Change, reported the following update:

Update - Change Healthcare is experiencing a network interruption related to a cyber security issue and our experts are working to address the matter. Once we became aware of the outside threat, in the interest of protecting our partners and patients, we took immediate action to disconnect our systems to prevent further impact. The disruption is expected to last at least through the day. We will provide updates as more information becomes available.²⁵

49. On February 28, 2024, BlackCat ransomware group, claimed responsibility for the Data Breach, revealing that they infiltrated Defendants' inadequately protected network and accessed several terabytes of highly sensitive information which was being kept unprotected.

50. On or around February 29, 2024, Defendant Change updated its Online Notice with the following information:

Update – Change Healthcare can confirm we are experiencing a cybersecurity issue perpetrated by a cybercrime threat actor who has represented itself to us as

²⁵ <https://status.changehealthcare.com/>. Although the initial notice posted is no longer active, a WayBack Machine archive version is accessible here: <https://web.archive.org/web/20240301000723/https://status.changehealthcare.com/> (last accessed May 9, 2024).

ALPHV/Blackcat. Our experts are working to address the matter and we are working closely with law enforcement and leading third-party consultants, Mandiant and Palo Alto Network, on this attack against Change Healthcare's systems.

We are actively working to understand the impact to members, patients and customers. Patient care is our top priority, and we have multiple workarounds to ensure people have access to the medications and the care they need. Based on our ongoing investigation, there's no indication that Optum, UnitedHealthcare and UnitedHealth Group systems have been affected by this issue.

We are working on multiple approaches to restore the impacted environment and continue to be proactive and aggressive with all our systems, and if we suspect any issue with the system, we will immediately take action.²⁶

51. Upon information and belief, the ransomware group BlackCat specifically targeted Defendants based on their status as healthcare entities with enormous amounts of valuable Private Information—including the Private Information of Plaintiffs' and Class Members' patients.

52. In response to the Data Breach, Defendants paid BlackCat a ransom of 350 bitcoins or roughly \$22 million on March 1, 2024.²⁷ It remains unclear to Plaintiffs and Class Members what the payment was for as, according to technology reporters, despite the payment of that ransom, Defendants "still face[] the risk of losing vast amounts of customers' sensitive medical data."²⁸

53. Two weeks after the Data Breach, on or around March 7, 2024, UnitedHealth Group released a statement: "We are working aggressively on the restoration of our systems and services."²⁹ Yet, over a month after the Data Breach, Defendants were only *beginning* "to test and

²⁶ *Id.*

²⁷ Andy Greenberg, Change Healthcare Finally Admits IT Paid Ransomware Hackers \$22 Million—and Still Faces a Patient Data Leak, *Wired* (Apr. 22, 2024) <https://www.wired.com/story/change-healthcare-admits-it-paid-ransomware-hackers/#:~:text=11%3A55%20PM-,Change%20Healthcare%20Finally%20Admits%20It%20Paid%20Ransomware%20Hackers%20%2422%20Million,up%20on%20the%20dark%20web>.

²⁸ *Id.*

²⁹ UnitedHealth Group Update on Change Healthcare Cyberattack, UnitedHealth Group, <https://www.unitedhealthgroup.com/newsroom/2024/2024-03-07-uhg-update-change-healthcare-cyberattack.html> (last accessed May 15, 2024).

reestablish”³⁰ connectivity to system services integral to Plaintiffs’ and Class Members’ ability to sustain their practices, including Defendants’ medical claims network and software.

54. As HIPAA covered business entities that collect, create, transfer, and maintain significant volumes of Private Information (through which roughly one-half of all America’s medical payments flow), the targeted attack was a foreseeable risk which Defendants were aware of, had previously and recently been affected by, and knew they had a duty to guard against. It is well-known that healthcare providers, such as Plaintiffs and Class Members, and their business associates, such as Defendants, which collect and store the confidential and sensitive Private Information of millions of individuals, are frequently targeted by cyberattacks. Further, cyberattacks are highly preventable through the implementation of reasonable and adequate cybersecurity safeguards, including proper employee cybersecurity training.

55. The Data Breach was the direct impetus for the subsequent outage of Defendant Change’s systems and services, which left Plaintiffs and Class Members unable to: verify patients’ insurance coverage; submit claims and receive payments; exchange clinical records; process prior authorization requests; generate cost estimates or bills; and generally provide healthcare services to their hundreds of millions of patients across the country.

56. The U.S. Department of Health and Human Services (“HHS”) and the Office of Consumer Rights urges HIPAA entities to encrypt data containing sensitive personal information. To underscore the necessity of doing so to protect consumers’ data, as far back as 2014, the Department fined two healthcare companies approximately two million dollars for failing to encrypt laptops containing sensitive personal information. In announcing the fines, Susan McAndrew, formerly OCR’s deputy director of health information privacy, stated that “[o]ur

³⁰ *ID.*

message to these organizations is simple: *encryption is your best defense against these incidents.*” Despite these fines and warnings, Defendants failed to encrypt the Private Information as recommended.

57. Defendants had obligations created by HIPAA, contract, industry standards, common law, and their own promises and representations made to Plaintiffs and Class Members to ensure their systems were adequately secured to keep Private Information confidential and were not maintained in a condition vulnerable to cyberattacks like the Data Breach.

58. Due to Defendants’ inadequate security measures and their decision to compound the harm by disconnecting all their revenue cycle services to Plaintiffs and Class Members, Defendants essentially guaranteed that no medical providers could be paid for the provision of healthcare services and/or handicapped the ability of medical providers to provide vital healthcare services to patients, in effect crippling the American healthcare system.

The Data Breach was a Foreseeable Risk of which Defendants Were on Notice

59. As HIPAA-covered entities handling Private Information, Defendants’ data security obligations were particularly important given the substantial increase in cyberattacks and data breaches in the healthcare industry and other industries holding significant amounts of PII and PHI preceding the Data Breach.

60. At all relevant times, Defendants knew, or should have known that their systems and networks were a target for malicious actors. As set forth *supra*, Defendants were recently the target of such an attack by malicious attackers and, subsequently, vowed to take the necessary and “immediate” steps to protect and safeguard Private Information. Yet, Defendants failed to implement and maintain reasonable and appropriate data privacy and security measures to protect their networks and the theft of Private Information from cyberattacks that Defendants knew

directly about and should have guarded against.

61. In addition to Defendants' own experience with a cyberattack in December 2022, Defendants knew or should have known from healthcare industry reports and studies identifying that cybercriminals target institutions which collect and store personal health information—like Defendants—at a greater rate than other sources of personal information. For example, in a 2022 report, the healthcare compliance company, Protenus, found that there were at least 905 health data breaches in 2021 alone, impacting over 50 million patients. The report noted that “the volume and impact of breaches continue to be underreported overall, and underrepresented to the public[,]” stressing that “gaps in detection and reporting mean the true impact of incidents is likely even greater.”³¹

62. The healthcare sector suffered at least 337 data breaches in the first half of 2022 alone, according to Fortified Health Security's mid-year report released in July 2022. The percentage of healthcare data breaches attributed to malicious activity rose more than five percentage points in the first six months of 2022 to account for nearly 80 percent of all reported incidents.³²

63. In light of the Defendants' own recent cybersecurity data breach and other high profile cybersecurity incidents at other healthcare partner and provider companies, including HCA Healthcare (11 million patients, July 2023), Managed Care of North America (8.8 patients, March 2023), Shields Health Care Group (2 million patients, March 2022), Broward Health (1.3 million

³¹ 2022 *Breach Barometer*, PROTENUS, https://www.protenus.com/hubfs/Breach_Barometer/BreachBarometer_Privacy_2022_Protenus.pdf?utm_campaign=Forbes%2520Articles&utm_source=forbes&utm_medium=article&utm_content=breach%2520barometer (last visited Dec. 11, 2023).

³² See Jill McKeon, *Health Sector Suffered 337 Healthcare Data Breaches in First Half of Year*, HEALTH IT SECURITY: CYBERSECURITY NEWS (July 19, 2022), <https://healthitsecurity.com/news/health-sector-suffered-337-healthcare-data-breaches-in-first-half-of-year>.

patients, January 2022), OneTouchPoint (2.6 million patients, July 2022), Trinity Health (3.3 million patients, May 2020), and American Medical Collection Agency (25 million patients, March 2019) Defendants knew or should have known that their electronic records would be targeted by cybercriminals.

64. PHI is particularly valuable and has been referred to as a “treasure trove for criminals.”³³ A cybercriminal who steals a person’s PHI can end up with as many as “seven to 10 personal identifying characteristics of an individual.”³⁴ A study by Experian found that the “average total cost” of medical identity theft was “about \$20,000” per incident in 2010, and that a majority of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.³⁵

65. In fact, according to the cybersecurity firm Mimecast, 90 percent of healthcare organizations experienced cyberattacks in 2020.³⁶

66. Cyberattacks on medical systems have become so common that in 2019 the FBI and U.S. Secret Service issued a warning to potential targets, so they are aware of, and prepared for, a potential attack. As one report explained, “[e]ntities like smaller municipalities and hospitals are attractive . . . because they often have lesser IT defenses and a high incentive to regain access

³³ See Andrew Steger, *What Happens to Stolen Healthcare Data?*, HEALTHTECH MAGAZINE (Oct. 30, 2019), <https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon> (quoting Tom Kellermann, Chief Cybersecurity Officer, Carbon Black, stating “Health information is a treasure trove for criminals.”).

³⁴ *Id.*

³⁵ Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (Mar. 3, 2010), <https://www.cnet.com/news/privacy/study-medical-identity-theft-is-costly-for-victims/>.

³⁶ See Maria Henriquez, *Iowa City Hospital Suffers Phishing Attack*, SECURITY MAGAZINE (Nov. 23, 2020), <https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack>.

to their data quickly.”³⁷

67. This was not the FBI’s first warning to the healthcare industry about the threat of cyberattacks. Indeed, cyberattacks against the healthcare industry have been common for over a decade, with the FBI warning as early as 2011 that cybercriminals were “advancing their abilities to attack a system remotely” and “[o]nce a system is compromised, cyber criminals will use their accesses to obtain PII[.]” The FBI further warned that “the increasing sophistication of cyber criminals will no doubt lead to an escalation in cybercrime.”³⁸ Later, in August 2014, after a cyberattack on Community Health Systems, Inc., the FBI warned companies within the healthcare industry that hackers were targeting them. The warning stated that “[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining the Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII).”

68. According to an article in the HIPAA Journal posted on November 2, 2023, cybercriminals hack into medical practices for their highly prized medical records. “[T]he number of data breaches reported by HIPAA-regulated entities continues to increase every year. 2021 saw 714 data breaches of 500 or more records reported to the [HHS’ Office for Civil Rights (OCR)] – an 11% increase from the previous year. Almost three-quarters of those breaches were classified as hacking/IT incidents.”³⁹

69. According to the HIPAA Journal’s 2023 Healthcare Data Breach Report, “[a]n

³⁷ FBI, *Secret Service Warn of Targeted Ransomware*, LAW360 (Nov. 18, 2019), <https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware>.

³⁸ Gordon M. Snow, *Statement before the House Financial Services Committee, Subcommittee on Financial Institutions and Consumer Credit*, FBI (Sept. 14, 2011), <https://archives.fbi.gov/archives/news/testimony/cyber-security-threats-to-the-financial-sector>.

³⁹ Steve Alder, *Editorial: Why Do Criminals Target Medical Records*, THE HIPAA JOURNAL (Nov. 2, 2023), <https://www.hipaajournal.com/why-do-criminals-target-medical-records>.

unwanted record was set in 2023 with 725 large security breaches in healthcare reported to the Department of Health and Human Services Office for Civil Rights, beating the record of 720 healthcare security breaches set the previous year.”⁴⁰

70. Healthcare organizations are easy targets because “even relatively small healthcare providers may store the records of hundreds of thousands of patients. The stored data is highly detailed, including demographic data, Social Security numbers, financial information, health insurance information, and medical and clinical data, and that information can be easily monetized.”⁴¹ In this case, Defendants failed to reasonably and adequately protect the stored records of *hundreds of millions* of patients—roughly one-third of all Americans.

71. The American Medical Association (“AMA”) has also warned healthcare companies about the importance of protecting their patients’ confidential information:

Cybersecurity is not just a technical issue; it’s a patient safety issue. AMA research has revealed that 83% of physicians work in a practice that has experienced some kind of cyberattack. Unfortunately, practices are learning that cyberattacks not only threaten the privacy and security of patients’ health and financial information, but also patient access to care.⁴²

72. Given Defendants’ own recent experience with a data breach and the wealth of information from law enforcement and the healthcare industry concerning the increasing prevalence of cyberattacks, Defendants knew and should have known about their data security

⁴⁰ Steve Adler, *Security Breaches in Healthcare in 2023*, The HIPAA Journal (January 31, 2024), https://www.hipaajournal.com/wp-content/uploads/2024/01/Security_Breaches_In_Healthcare_in_2023_by_The_HIPAA_Journal.pdf.

⁴¹ *See id.*

⁴² Andis Robeznieks, *Cybersecurity: Ransomware attacks shut down clinics, hospitals*, AM. MED. ASS’N (Oct. 4, 2019), <https://www.ama-assn.org/practice-management/sustainability/cybersecurity-ransomware-attacks-shut-down-clinics-hospitals>.

vulnerabilities and implemented enhanced and adequate protection to protect and secure Private Information.

73. Despite knowing the risks, Defendants failed to enhance their security, which resulted in the Data Breach, and ultimately in Defendants' ensuing decision to disconnect Change's services to medical providers like Plaintiffs and Class Members in the aftermath of the Data Breach.

Defendants Failure to Comply with FTC Guidelines

74. The Federal Trade Commission ("FTC") has regularly promulgated guidelines for businesses, including HIPAA entities, which highlight the necessity of implementing reasonable data security practices. According to the FTC, the need for data security should factor into all business decision-making.

75. For example, in 2016, the FTC updated its published guidelines, *Protecting Personal Information: A Guide for Business*, which laid out standard and accepted cyber-security measures for businesses to implement to protect consumers' private data. The guidelines advise businesses, *inter alia*, to: encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.⁴³

76. The FTC's guidelines further advise businesses: not to maintain PII longer than necessary for authorization of a transaction; to limit access to sensitive data; to require complex passwords to be used on networks; to use industry-tested methods for security; to monitor for suspicious activity on the network; and to verify that third-party service providers have implemented reasonable security measures.

⁴³ *Protecting Personal Information: A Guide for Business*, FEDERAL TRADE COMMISSION (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

77. To underscore the binding significance of the promulgated guidance, the FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, pursuant to Section 5 of the Federal Trade Commission Act (“FTCA”), 15 U.S.C. § 45. Orders resulting from these actions further identify the measures businesses *must* take to meet their data security obligations consistent with federal law.

78. These FTC enforcement actions include actions against healthcare providers and partners like Defendants. *See, e.g., In the Matter of LabMD, Inc., A Corp.*, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) (“[T]he Commission concludes that LabMD’s data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.”).

79. Defendants’ failure to employ reasonable and appropriate measures to protect against unauthorized access to patients’ Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

80. Defendants were at all times fully aware of their obligations to protect the Private Information of customers and patients. Defendants were also aware of the significant repercussions that would result from their failure to do so.

Defendants Failure to Comply with Accepted Industry Standards for Data Security

81. In light of the evident threat of cyberattacks seeking consumers’ Private Information, several best practices have been identified by regulatory agencies and experts that, at a minimum, should be implemented by healthcare service providers like Defendants to secure Private Information, including but not limited to: educating and training all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data;

monitoring and limiting the network ports; protecting web browsers and email management systems; and limiting which employees can access sensitive data.

82. On information and belief, Defendants failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

83. These foregoing frameworks are existing and applicable industry standards in the healthcare industry, and Defendants failed to comply with these accepted standards, thereby opening the door to the Data Breach.

**Defendants Failure to Comply with Their
HIPAA Obligations to Safeguard Private Information**

84. As a healthcare service provider handling medical patient data and providing services to hospitals and healthcare organizations, Defendants are covered entities under HIPAA (45 C.F.R. § 160.103) and are required to comply with the HIPAA Privacy Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and C ("Security Standards for the Protection of Electronic Protected Health Information").

85. HIPAA requires covered entities to protect against reasonably anticipated threats to the security of sensitive patient health information.

86. Defendants are subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act ("HITECH"). *See* 42 U.S.C. § 17921, 45 C.F.R. § 160.103.

87. HIPAA's Privacy Rule or *Standards for Privacy of Individually Identifiable Health Information* establishes national standards for the protection of health information that is kept or transferred in electronic form.

88. HIPAA covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. These Safeguards include physical, technical, and administrative components.

89. The Data Breach is considered a breach under the HIPAA Rules because it involved an access of PHI not permitted under the HIPAA Privacy Rule:

A breach under the HIPAA Rules is defined as "the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI." *See* 45 C.F.R. 164.40

90. The Data Breach resulted from a combination of multiple failures by the Defendants to adequately and reasonably secure the Private Information in violation of the mandates set forth in in HIPAA's regulations, and the harm suffered by Plaintiffs and Class Members flowed directly from these failures by the Defendants and their decision following the Data Breach to disconnect their services to Plaintiffs and Class Members.

Defendants' Failure to Adequately and Reasonably Protect Against the Data Breach was Reckless and Negligent

91. Defendants breached their obligations to Plaintiffs and Class Members and/or were otherwise negligent and reckless because they failed to properly maintain and safeguard their computer systems and data to protect and safeguard stored Private Information., which ultimately culminated in their taking all of Defendant Change's services offline to the detriment of Plaintiffs and Class Members. Defendants' unlawful conduct includes, but is not limited to, the following acts and/or omissions:

- a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;
- b. Failing to adequately protect patients' and customers' Private Information;
- c. Failing to properly monitor their own data security systems for existing intrusions;
- d. Failing to ensure that their vendors with access to their computer systems and data employed reasonable security procedures;
- e. Failing to train their employees in the proper handling of emails containing Private Information and maintain adequate email security practices;
- f. Failing to ensure the confidentiality and integrity of electronic PHI they created, received, maintained, and/or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);
- g. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);
- h. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. § 164.308(a)(1)(i);
- i. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);
- j. Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. §

164.306(a)(2);

- k. Failing to protect against reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);
- l. Failing to ensure compliance with HIPAA security standard rules by their workforces in violation of 45 C.F.R. § 164.306(a)(4);
- m. Failing to train all members of their workforces effectively on the policies and procedures regarding PHI as necessary and appropriate for the members of their workforces to carry out their functions and to maintain security of PHI, in violation of 45 C.F.R. § 164.530(b);
- n. Failing to render the electronic Private Information they maintained unusable, unreadable, or indecipherable to unauthorized individuals, as they had not encrypted the electronic PHI as specified in the HIPAA Security Rule by “the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key” (45 CFR § 164.304’s definition of “encryption”);
- o. Failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act; and
- p. Failing to adhere to industry standards for cybersecurity as discussed above.

92. Defendants negligently, recklessly, and unlawfully failed to the Private Information of Plaintiffs’ and Class Members’ patients by allowing cyberthieves to access

Defendants' computer network and systems which contained unsecured and unencrypted Private Information, and are now making Plaintiffs and Class Members pay the price.

93. Healthcare providers and practices, like Plaintiffs' and Class Members', were and continue to not receive the services they paid Defendants for. As a result, Plaintiffs and Class Members are struggling to care for patients, are losing money, and are having to rely on their personal savings to continue to provide vital healthcare services to millions of Americans across the country and face the specter of continued financial hardship Defendants' failures have caused.

94. Accordingly, as outlined below, Plaintiffs and Class members now face the risk of permanent closure. In addition, Plaintiffs and Class Members also lost the benefit of their bargain with Defendants.

Plaintiffs' Damages and Experiences

95. Beginning on or around February 21, 2024, when Defendants' systems were shut down as a result of the Data Breach, Plaintiffs have been unable to bill electronically for the services they have been providing to patients. As a result, Plaintiffs estimate they have lost approximately \$15,000 in roughly two months alone. As of the date of this filing, Plaintiffs are still suffering financial harm and are approximately two months behind on collecting revenue they are due.

96. Ordinarily, Plaintiffs process their claims on a daily basis through their third-party practice management services provider CompuGroup Medical, which deals directly with Change. However, in the aftermath of the Data Breach Plaintiffs were unable to receive revenue for the services they provide to patients daily.

97. Moreover, following the Data Breach, there was no direct communication to Plaintiffs from Change that there had been a cyberattack and that the claims they sent out were not

being processed. Instead, Plaintiffs were entirely in the dark until they learned about the Data Breach on their own from news stories that had been published.

98. Because of this substantial loss of cash flow resulting from the Data Breach, Plaintiff Shillito has had to take out a \$25,000 personal loan, just to keep the practice she co-owns afloat, and to ensure that the practice is able to continue to provide vital medical services to the patients they serve.

99. In addition to the financial harm suffered by Plaintiffs from their inability to bill electronically, having to take out a personal loan to save her business and serve her patients has caused Plaintiff Shillito to suffer significant emotional distress. Plaintiff Shillito is enduring severe stress, insomnia, anxiety, and other health issues stemming from Defendants' conduct related to the Data Breach and their ensuing decision to disconnect Change's services to healthcare practices and providers. Plaintiffs' entire practice staff continues to feel daily uncertainty over their revenue, and the Parker Medical Practice LPD's sole physician, Plaintiff Shillito's spouse, took a significant pay reduction following the Data Breach just to ensure the practice's other six staff member could be paid. As a result, Plaintiff Shillito is behind on her personal financial obligations.

100. As a direct and proximate result of Defendants' actions and inactions, Plaintiffs and Class Members have suffered anxiety, emotional distress, and loss of revenue.

CLASS ACTION ALLEGATIONS

101. Plaintiffs bring this action against Defendants individually and on behalf of all other persons similarly situated.

102. Plaintiffs propose the following Class definition, subject to amendment as appropriate:

**All healthcare providers and practices in the United States
whose use of Change Healthcare's services was disrupted by the**

Data Breach (the “Class”).

103. Excluded from the Class are Defendants’ officers, directors, and employees; any entity in which Defendants have a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendants. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families and members of their staff.

104. Plaintiffs reserve the right to amend or modify the Class or Subclass definition or create additional subclasses as this case progresses.

105. Numerosity. The Members of the Class are so numerous that joinder of all of them is impracticable. The CEO of Defendant UnitedHealth Group, Andrew Witty, estimates that as many as *one-third of all Americans* may have been impacted by the Data Breach—comprising of patients of a substantial number of healthcare providers and practices nationwide.

106. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

- a. Whether Defendants failed to implement and maintain reasonable and adequate security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
- b. Whether Defendants’ data security systems prior to and during the Data Breach complied with applicable data security laws and regulations including, e.g., HIPAA;
- c. Whether Defendants’ data security systems prior to and during the Data Breach were consistent with industry standards;
- d. Whether Defendants knew or should have known that their data security

systems and monitoring processes were deficient;

- e. Whether Defendants should have discovered the Data Breach sooner;
- f. Whether Plaintiffs and Class Members suffered legally cognizable damages as a result of Defendants' misconduct;
- g. Whether Defendants' conduct was negligent;
- h. Whether Defendants breached contracts with Plaintiffs and Class Members;
- i. Whether Defendants were unjustly enriched by unlawfully retaining a benefit conferred upon them by Plaintiffs and Class Members;
- j. Whether Defendants failed to provide notice of the Data Breach in a timely manner, and;
- k. Whether Plaintiffs and Class Members are entitled to damages, civil penalties, punitive damages, treble damages, and/or injunctive relief.

107. Typicality. Plaintiffs' claims are typical of those of other Class Members because Plaintiffs, like all other Class Members, suffered financial and other harm as a result of the Data Breach and ensuing shutdown of Defendants' networks and systems.

108. Adequacy of Representation. Plaintiffs will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiffs' Counsel are competent and experienced in litigating class actions.

109. Predominance. Defendants have engaged in a common course of conduct toward Plaintiffs and Class Members, in that Defendants' Data Breach and ensuing system shutdown affected all Class Members in the same way. The common issues arising from Defendants' conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of

judicial economy.

110. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendants. In contrast, to conduct this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

111. Defendants have acted on grounds that apply generally to the Class as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

112. Likewise, particular issues are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

- a. Whether Defendants' security measures to protect their data systems were reasonable and adequate in light of best practices recommended by data security experts;
- b. Whether Defendants' failure to institute adequate protective security measures amounted to negligence;
- c. Whether Defendants failed to take commercially reasonable steps to prevent

the Data Breach; and

- d. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

113. Finally, all members of the proposed Class are readily ascertainable. Defendants have access to Class Members' names and addresses affected by the Data Breach as they are customers of Defendants.

CLAIMS FOR RELIEF

COUNT I

Negligence

(On Behalf of Plaintiffs and the Class)

114. Plaintiffs re-allege and incorporate by reference all factual allegations above as if fully set forth herein.

115. At all times relevant hereto, Defendants owed Plaintiffs and Class Members a duty to act with reasonable care to ensure continuity of their Defendants' networks systems and to ensure that their financial and payment services would be adequately performed, including by way of timely and accurate claims processing. Defendants assumed this obligation and Defendants owed a duty of care to Plaintiffs and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that their systems and networks, and the personnel responsible for them, adequately protected their network and systems from attack by malicious actors.

116. Plaintiffs and Class Members are a well-defined, foreseeable, and probable group of healthcare and medical providers and practices that Defendants were aware, or should have been aware, could be injured by inadequate data security measures.

117. Defendants’ duty of care to use reasonable and adequate security measures arose as a result of Defendants’ role as a provider of integral technology, insurance, and revenue cycle services to healthcare providers and which is recognized by laws and regulations including but not limited to HIPAA, the FTC Act, and common law. Defendants were in a superior position to ensure that their systems were sufficient to protect against the foreseeable risk of harm to Plaintiffs and Class Members from a data breach and any ensuing need of Defendants to disconnect their services to Plaintiffs and Class Members.

118. Defendants’ duty to use reasonable security measures under HIPAA required Defendants to “reasonably protect” confidential data from “any intentional or unintentional use or disclosure” and to “have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information.” 45 C.F.R. § 164.530(c)(1). Some or all of the medical information at issue in this case constitutes “protected health information” within the meaning of HIPAA.

119. In addition, Defendants had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits “unfair... practices in or affecting commerce,” including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

120. Defendants’ duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendants are bound by industry standards to protect confidential private information.

121. Moreover, it was reasonably foreseeable to Defendants that Plaintiffs and Class Members would suffer such harms in the event of a cyberattack such as the Data Breach which required Defendants to disconnect their systems and cease their provision of services to Plaintiffs

and Class Members.

122. Defendants breached their duties, and thus were negligent, by failing to use reasonable measures to protect their systems from a Data Breach. The specific negligent acts and omissions committed by Defendants include, but are not limited to, the following:

- a. Failing to adopt, implement, and maintain reasonable and adequate security measures to safeguard their networks, systems, and servers;
- b. Failing to adequately monitor the security of their networks and systems;
- c. Failing to ensure that their email systems had reasonable data security safeguards in place;
- d. Failing to have in place reasonable and adequate mitigation policies and procedures;
- e. Failing to detect in a timely manner that there had been an exploitation of their security vulnerabilities;
- f. Failing to timely notify Plaintiffs and Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential harm;
- g. Failing to have a plan to mitigate harm to healthcare and medical practices and providers like Plaintiffs and Class Members in the event of a cyberattack like the Data Breach; and
- h. Causing the Change Healthcare outage which left Plaintiffs and Class Members with no ability to verify patients' insurance coverage, submit claims and receive payments, exchange clinical records, generate cost estimates and bills, or process prior authorization requests.

123. Plaintiffs and Class Members have no ability to protect their access to Defendants'

systems and services, and it remains in Defendants' sole discretion when they will restore their full suite of services to Plaintiffs and Class Members.

124. It was foreseeable that Defendants' failure to use reasonable measures to protect their networks and systems, and Defendants' decision to take their services to healthcare and medical providers and practices offline, would result in injury to Plaintiffs and Class Members. Furthermore, the breach of security was reasonably foreseeable given the prior breach of Defendants' own data systems, the known high frequency of cyberattacks and data breaches in the healthcare industry.

125. It was therefore foreseeable that the failure to adequately secure the Private Information stored in their systems and networks would result in one or more types of injuries to Plaintiffs and Class Members, including the financial injury that resulted from Defendants' decision to disconnect Change from the rest of the healthcare system.

126. Defendants' conduct was grossly negligent and departed from reasonable standards of care, including but not limited to, failing to adequately protect their systems and networks from a cyberattack and depriving Plaintiffs and Class members of access to the services necessary for them to sustain their practices and continue to provide vital care to their patients.

127. Neither Plaintiffs nor Class Members contributed to the Data Breach and subsequent harm endured as a result of the Data Breach and Defendants' ensuing decision to disconnect Change from the rest of the healthcare system.

128. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendants to, *e.g.*, (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to recompense Plaintiffs and Class Members for all financial losses suffered as a result of the Change

outage.

129. The injury and harm Plaintiffs and Class Members suffered was the reasonably foreseeable result of Defendants' breach of their duties. Defendants knew or should have known that they were failing to meet their duties, and that Defendants' breach would cause Plaintiffs and Class Members to experience the foreseeable harms associated with the Data Breach and ensuing Change outage.

130. As a direct and proximate result of Defendants' negligent conduct, Plaintiffs and Class Members have suffered injury and are entitled to compensatory and consequential damages in an amount to be proven at trial.

COUNT II
Breach of Implied Contract
(On behalf of Plaintiffs and the Class)

131. Plaintiffs re-allege and incorporate by reference all factual allegations above as if fully set forth herein.

132. Defendants acquired and maintained the Private Information of Plaintiffs and the Class Members' patients that they received either directly or from Plaintiffs and the Class Members.

133. Defendants including Defendant Change entered into contracts with Plaintiffs and Class Members. Specifically, When Plaintiffs and Class Members paid money to Defendants for their services, either directly or indirectly, in exchange for goods or services, they entered into contracts Defendants.

134. Defendants directly or indirectly solicited, offered, and invited Plaintiffs and Class Members to provide their patients' Private Information as part of Defendants' regular business practices. Plaintiffs and Class Members accepted Defendants offers and provided their patients'

Private Information to Defendants.

135. Defendants accepted possession of Plaintiffs and Class Members' patients' Private Information for the purpose of providing services to Plaintiffs and Class Members.

136. In accepting such information and payment for services, Defendants entered into implied contracts with Plaintiffs and Class Members whereby Defendants became obligated to reasonably safeguard the Private Information.

137. Implicit in the contracts were Defendants' obligations to reasonably safeguard the Private Information stored in its systems from cyberattack, including ransomware attacks.

138. In delivering their patients' Private Information to Defendants and paying for Defendants' services, Plaintiffs and Class Members intended and understood that Defendants would adequately safeguard the Private Information as part of that service and would not suffer service disruptions for failure to do so.

139. The implied promise of confidentiality includes consideration beyond those pre-existing general duties owed under HIPAA or other state or federal regulations. The additional consideration included implied promises to take adequate steps to comply with specific industry data security standards and FTC guidelines on data security.

140. The implied promises include but are not limited to: (1) taking steps to ensure that any agents who are granted access to Private Information also protect the confidentiality of that data; (2) taking steps to ensure that the information that is placed in the control of their agents is restricted and limited to achieve an authorized medical purpose; (3) restricting access to qualified and trained agents; (4) designing and implementing appropriate retention policies to protect the information against criminal data breaches; (5) applying or requiring proper encryption; (6) multifactor authentication for access; and (7) other steps to protect against foreseeable data

breaches.

141. Plaintiffs and Class Members would not have entrusted their patients' Private Information to Defendants in the absence of such an implied contract.

142. Had Defendants disclosed to Plaintiffs and Class Members that they did not have adequate computer systems and security practices to secure sensitive data, Plaintiffs and Class Members would not have provided their patients' Private Information to Defendants.

143. Defendants recognized that Plaintiffs' and Class Members' Private Information is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain with Plaintiffs and Class Members.

144. Plaintiffs and Class Members fully performed their obligations under the implied contracts with Defendants.

145. Defendants breached the implied contracts with Plaintiffs and Class Members by failing to take reasonable and adequate measures to safeguard their patients' Private Information as described herein.

146. As a direct and proximate result of Defendants' conduct, Plaintiffs and Class Members suffered and will continue to suffer actual losses and damages in an amount to be proven at trial.

COUNT III
Breach of Third-Party Beneficiary Contract
(On Behalf of Plaintiffs and the Class)

147. Plaintiffs incorporate and reallege all factual allegations above as if fully set forth herein.

148. This allegation is pled in the alternative to Count II.

149. Defendants entered into a contract to provide services to Plaintiffs' practice

management services provider or other third-party providers contracted by Plaintiffs and the Class, which in turn, contracted directly with Defendant Change to obtain revenue cycle services. Upon information and belief, this contract is virtually identical to the contracts entered into between Defendants and other third-party healthcare revenue service providers around the country serving medical practices that were also affected by the Data Breach.

150. These contracts were made expressly for the benefit of Plaintiffs and the Class, as it was their revenue that Defendants agreed to reimburse through these healthcare practice management providers, based on the services provided by Plaintiffs and the Class to their patients. Thus, the benefit of paying this revenue to Plaintiffs and the Class for the medical services they provided to patients was the direct and primary objective of the contracting parties.

151. Defendants knew that if they were to breach these contracts with its customers, the customers' clients, including Plaintiffs and the Class, would be harmed by, among other harms, financial losses.

152. Defendants breached their contracts with providers or practice management and/or revenue cycle services affected by this Data Breach when they failed to use reasonable data security measures that could have prevented the Data Breach, and subsequently disconnected the healthcare services provided by Defendant Change.

153. As foreseen, Plaintiffs and the Class were harmed by Defendants' failure to use reasonable security measures to store patient information, and their subsequent decision to disconnect Change's services to medical providers and their third-party contractors.

154. Accordingly, Plaintiffs and the Class are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

COUNT IV
Unjust Enrichment
(On Behalf of Plaintiffs and the Class)

155. Plaintiffs reallege and incorporate by reference all factual allegations above as if fully set forth herein.

156. This count is pleaded in the alternative to the breach of contract claims (Counts II and III).

157. Upon information and belief, Defendants fund any data security measures they implement entirely from their general revenue, including from money they make based upon representations of Protecting Plaintiffs' and Class Members' patients' Private Information.

158. There is a direct nexus between money paid to Defendants and the requirement that Defendants adequately secure their computer networks and adopt sufficient data security practices to safeguard and protect Private Information.

159. Plaintiffs and Class Members paid Defendants a certain sum of money, which was used to fund any data security measures implemented by Defendants via contracts with Defendants.

160. As such, a portion of the payments made by or on behalf of Plaintiffs and Class Members is to be used to provide a reasonable and adequate level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendants.

161. Ensuring their computer systems are secure and can continually provide services to Plaintiffs and Class Members without interruption or outage is an integral part of Defendants' businesses.

162. Plaintiffs and Class Members directly and indirectly conferred a monetary benefit on Defendants. Specifically, they purchased goods and services from Defendants and/or their

agents and provided Defendants with their claims processing and revenue cycle service materials and their patients' data. In exchange, Plaintiffs and Class Members should have received from Defendants the goods and services that were the subject of the transaction and have their processing and service materials protected with adequate data security.

163. Defendants knew that Plaintiffs and Class Members conferred a benefit which Defendants accepted. Defendants profited from these transactions—to the tune of \$324 billion in revenue in 2023 alone — and used the money paid by Plaintiffs and Class Members for business purposes.

164. Defendants enriched themselves by saving the costs they reasonably should have expended on adequate data security measures to secure their servers and networks and prevent the need for a systemwide outage and interruption of services to Plaintiffs and Class Members. Instead of providing a reasonable and adequate level of security that would have prevented the Data Breach, Defendants instead chose to shirk their data security obligations to increase profits at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective data security measures. Plaintiffs and Class Members suffered as a direct and proximate result of Defendants' calculated failures to provide the requisite reasonable and adequate data security.

165. Under the principles of equity and good conscience, Defendants should not be permitted to retain the money belonging to Plaintiffs and Class Members, because Defendants failed to implement reasonable and adequate data management and security measures that are mandated by federal law and industry standards.

166. Defendants acquired the monetary benefit and Private Information through inequitable means in that they failed to disclose the inadequate security practices previously alleged.

167. Plaintiffs and Class Members have no adequate remedy at law.

168. As a direct and proximate result of Defendants' conduct, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

169. Defendants should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that they unjustly received from them. In the alternative, Defendants should be compelled to refund the amounts that Plaintiffs and Class Members overpaid for Defendants' services.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs pray for judgment as follows:

- a) For an Order certifying this action as a Class Action and appointing Plaintiffs as Class Representatives and their counsel as Class Counsel;
- b) For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiffs and Class Members;
- c) For equitable relief compelling Defendants to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of Private Information compromised during the Data Breach;
- d) For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendants' wrongful conduct;
- e) Ordering Defendants to pay for not less than five years of credit monitoring services for Plaintiffs and the Class;
- f) For an award of actual damages, compensatory damages, statutory damages,

nominal damages, and/or statutory penalties, in an amount to be determined, as allowable by law;

- g) For an award of punitive damages, as allowable by law;
- h) Pre- and post-judgment interest on any amounts awarded; and,
- i) Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

Under Federal Rule of Civil Procedure 38(b), Plaintiffs demand a trial by jury of any and all issues in this action so triable as of right.

Dated: May 16, 2024

Respectfully submitted,

/s/ J. Gerard Stranch IV

J. Gerard Stranch, IV, BPR 23045

Grayson Wells BPR 039658

**STRANCH, JENNINGS & GARVEY
PLLC**

The Freedom Center

223 Rosa L. Parks Avenue, Suite 200

Nashville, Tennessee 37203

Tel: (615) 254-8801

gstranch@stranchlaw.com

gwells@stranchlaw.com

James J. Pizzirusso*

Nicholas Murphy*

Mandy Boltax*

HAUSFELD LLP

888 16th Street, N.W., Suite 300

Washington, D.C. 20006

(202) 540-7200

jpizzirusso@hausfeld.com

nmurphy@hausfeld.com

mboltax@hausfeld.com

Steven M. Nathan*

Ashley Crooks*

HAUSFELD LLP

33 Whitehall Street, Fourteenth Floor

New York, NY 10004

(646) 357-1100
snathan@hausfeld.com
acrooks@hausfeld.com

Counsel for Plaintiffs

****Pro Hac Vice Forthcoming***